

1. In computer network interconnecting a client system, a proxy system, and a
2 server system, wherein data exchanged over the computer network is subject to being
3 compromised, a method of negotiating, through the proxy system, a secure end-to-end
4 connection between the client system and the server system, wherein the client system
5 securely authenticates to the proxy system, the method comprising the acts of:

6 receiving a request from the client system for a secure connection between
7 the client system and the proxy system;

8 establishing a secure connection between the client and proxy systems;

9 receiving a request from the client system for a secure end-to-end connection
10 with the server system;

11 forwarding the client system request for a secure end-to-end connection to the
12 server system; and

13 downgrading the secure connection between the client system and the proxy
14 system to be insecure after the secure end-to-end connection is established, whereby
15 the secure end-to-end connection is encapsulated within the insecure client-proxy
16 connection.

17
18 2. A method as recited in claim 1 further comprising the acts of:

19 issuing an authenticate challenge to the client system; and

20 receiving, over the secure client-proxy connection, proper authentication
21 credentials from the client system.

22
23 3. A method as recited in claim 2 wherein the authenticate challenge issued to
24 the client system is one of a basic and a digest authenticate challenge.

1 4. A method as recited in claim 1 wherein at least one of the secure client-proxy
2 connection and the secure end-to-end connection is certificate based.

3
4 5. A method as recited in claim 4 wherein at least one of the secure client-proxy
5 connection and the secure end-to-end connection is one of a secure sockets layer and a
6 transport layer security connection.

7
8 6. A method as recited in claim 1 further comprising the act of sending a
9 certificate to the client system, wherein the certificate may be used to verify the identity of
10 the proxy system.

11
12 7. A method as recited in claim 1 further comprising the act of receiving proper
13 authentication credentials from the client system, wherein the proper authentication
14 credentials received from the client system are certificate based.

15
16 8. A method as recited in claim 1 further comprising the act of transferring data
17 between the client system and the server system through the secure end-to-end connection.

18
19 9. A method as recited in claim 1 wherein downgrading the secure connection
20 between the client system and the proxy system to be insecure comprises the act of setting
21 the cipher set for the connection to be a null cipher.

22
23 10. A method as recited in claim 1 wherein the request for a secure end-to-end
24 connection comprises a hypertext transfer protocol connect request.

1 11. A method as recited in claim 1 wherein the server system comprises one of a
2 reverse proxy server system and a forward proxy system.

3
4 12. A method as recited in claim 1 wherein at least one connection is over the
5 Internet.

6
7 13. A method as recited in claim 1 wherein the server system comprises a
8 cascaded proxy system, the server system allowing secure connections, insecure
9 connections, or both secure and insecure connections, with one or more other server
10 systems.

1 14. In computer network interconnecting a client system, a proxy system, and a
2 server system, wherein data exchanged over the computer network is subject to being
3 compromised, a method of negotiating, through the proxy system, a secure end-to-end
4 connection between the client system and the server system, wherein the client system
5 securely authenticates to the proxy system, the method comprising the acts of:

6 sending a request to the proxy system for a secure connection between the
7 client system and the proxy system;

8 establishing a secure connection between the client and proxy systems;

9 sending a request to the proxy system for a secure end-to-end connection
10 with the server system;

11 downgrading the secure connection between the client system and the proxy
12 system to be insecure after the secure end-to-end connection is established, whereby
13 the secure end-to-end connection is encapsulated within the insecure client-proxy
14 connection.

15. A method as recited in claim 14 further comprising the acts of:

17 receiving an authenticate challenge from the proxy system; and

18 sending, over the secure client-proxy connection, proper authentication
19 credentials to the proxy system.

21 16. A method as recited in claim 15 wherein the authenticate challenge received
22 by the client system is one of a basic and a digest authenticate challenge.

1 17. A method as recited in claim 14 wherein at least one of the secure
2 client-proxy connection and the secure end-to-end connection is certificate based.

3
4 18. A method as recited in claim 17 wherein at least one of the secure
5 client-proxy connection and the secure end-to-end connection is one of a secure sockets
6 layer and a transport layer security connection.

7
8 19. A method as recited in claim 14 further comprising the act of receiving a
9 certificate from the proxy system, wherein the certificate may be used to verify the identity
10 of the proxy system.

11
12 20. A method as recited in claim 14 further comprising the act of sending proper
13 authentication credentials to the proxy system, wherein the proper authentication credentials
14 sent to the proxy system are certificate based.

15
16 21. A method as recited in claim 14 further comprising the act of transferring
17 data to the server system through the secure end-to-end connection.

18
19 22. A method as recited in claim 14 wherein downgrading the secure connection
20 between the client system and the proxy system to be insecure comprises the act of setting
21 the cipher set for the connection to be a null cipher.

22
23 23. A method as recited in claim 14 wherein the request for a secure end-to-end
24 connection comprises a hypertext transfer protocol connect request.

1 24. A method as recited in claim 14 wherein the server system comprises one of
2 a reverse proxy server system and a forward proxy server system.

3
4 25. A method as recited in claim 14 wherein at least one connection is over the
5 Internet.

6
7 26. A method as recited in claim 14 wherein the server system comprises a
8 cascaded proxy system, the server system allowing secure connections, insecure
9 connections, or both secure and insecure connections, with one or more other server
10 systems.

1 27. In computer network interconnecting a client system, a proxy system, and a
2 server system, wherein data exchanged over the computer network is subject to being
3 compromised, a method of negotiating, through the proxy system, a secure end-to-end
4 connection between the client system and the server system, wherein the client system
5 securely authenticates to the proxy system, the method comprising steps for:

6 negotiating a secure connection between the client and proxy systems;
7 negotiating a secure end-to-end connection between the client and the server
8 system using the secure client-proxy connection;
9 altering the secure client-proxy connection so that it is no longer secure; and
10 encapsulating the secure end-to-end connection within the insecure
11 client-proxy connection.

12
13 28. A method as recited in claim 27 further comprising a step for authenticating
14 the client system to the proxy system, wherein the step for authenticating comprises an act
15 of either the client system sending or the proxy system receiving, proper authentication
16 credentials including at least one of a basic authenticate challenge response, a digest
17 authenticate challenge response, and a certificate.

18
19 29. A method as recited in claim 27 wherein the step for negotiating a secure
20 connection between the client and proxy systems comprises the act of the client system
21 receiving or the proxy system sending a certificate, wherein the certificate may be used to
22 verify the identity of the proxy system.

1 30. A method as recited in claim 27 wherein at least one of the secure
2 client-proxy connection and the secure end-to-end connection is certificate based.

3
4 31. A method as recited in claim 30 wherein at least one of the secure
5 client-proxy connection and the secure end-to-end connection is one of a secure sockets
6 layer and a transport layer security connection.

7
8 32. A method as recited in claim 27 wherein the step for altering the secure
9 client-proxy connection comprises the act of setting the cipher set for the connection to be a
10 null cipher, thereby downgrading the client-proxy connection to be insecure.

11
12 33. A method as recited in claim 27 where the step for negotiating a secure
13 end-to-end connection comprises the act of either the client system sending or the proxy
14 system receiving a hypertext transfer protocol connect request.

15
16 34. A method as recited in claim 27 wherein the server system comprises a
17 cascaded proxy system, the server system allowing secure connections, insecure
18 connections, or both secure and insecure connections, with one or more other server
19 systems.

1 35. In computer network interconnecting a client system, a proxy system, and a
2 server system, wherein data exchanged over the computer network is subject to being
3 compromised, a computer program product for implementing a method of negotiating,
4 through the proxy system, a secure end-to-end connection between the client system and the
5 server system, wherein the client system securely authenticates to the proxy system,
6 comprising:

7 a computer readable medium for carrying machine-executable instructions
8 for implementing the method; and

9 wherein said method is comprised of machine-executable instructions for a
10 proxy system performing the acts of:

11 receiving a request from the client system for a secure connection
12 between the client system and the proxy system;

13 establishing a secure connection between the client and proxy
14 systems;

15 receiving a request from the client system for a secure end-to-end
16 connection with the server system;

17 forwarding the client system request for a secure end-to-end
18 connection to the server system; and

19 downgrading the secure connection between the client system and the
20 proxy system to be insecure after the secure end-to-end connection is
21 established, whereby the secure end-to-end connection is encapsulated within
22 the insecure client-proxy connection.

1 36. A computer program product as recited in claim 35, the method comprised
2 further of machine-executable instructions for performing the acts of:

- 3 issuing an authenticate challenge to the client system; and
- 4 receiving proper authentication credentials from the client system.

6 37. A computer program product as recited in claim 36 wherein the authenticate
7 challenge issued to the client system is one of a basic and a digest authenticate challenge.

9 38. A computer program product as recited in claim 36, the method comprised
10 further of machine executable instructions for performing the act of sending a certificate to
11 the client system, wherein the certificate may be used to verify the identity of the proxy
12 system.

14 39. A computer program product as recited in claim 36 wherein at least one of
15 the secure client-proxy connection and the secure end-to-end connection is certificate based.

17 40. A computer program product as recited in claim 39 wherein at least one of
18 the secure client-proxy connection and the secure end-to-end connection is one of a secure
19 sockets layer and a transport layer security connection.

21 41. A computer program product as recited in claim 35, the method further
22 comprised of machine-executable instructions for performing the act of receiving proper
23 authentication credentials from the client system, wherein proper authentication credentials
24 received from the client system are certificate based.

1 42. A computer program product as recited in claim 35, the method further
2 comprised of machine-executable instructions for performing the act of transferring data
3 between the client system and the server system through the secure end-to-end connection.

4

5 43. A computer program product as recited in claim 35, the method comprised
6 further of machine-executable instructions for performing the act of setting the cipher set for
7 the secure client-proxy connection to be a null cipher, thereby downgrading the client-proxy
8 connection to be insecure.

9

10 44. A computer program product as recited in claim 35 wherein the request for a
11 secure end-to-end connection comprises a hypertext transfer protocol connect request.

12

13 45. A computer program product as recited in claim 35 wherein the server system
14 comprises one of a reverse proxy server system and a forward proxy server system.

15

16 46. A computer program product as recited in claim 35 wherein at least one
17 connection is over the Internet.

18

19 47. A computer program product as recited in claim 35 wherein the server system
20 comprises a cascaded proxy system, the server system allowing secure connections, insecure
21 connections, or both secure and insecure connections, with one or more other server
22 systems.

1 48. In computer network interconnecting a client system, a proxy system, and a
2 server system, wherein data exchanged over the computer network is subject to being
3 compromised, a computer program product for implementing a method of negotiating,
4 through the proxy system, a secure end-to-end connection between the client system and the
5 server system, wherein the client system securely authenticates to the proxy system,
6 comprising:

7 a computer readable medium for carrying machine-executable instructions
8 for implementing the method; and

9 wherein said method is comprised of machine-executable instructions for a
10 client system performing the acts of:

11 sending a request to the proxy system for a secure connection between
12 the client system and the proxy system;

13 establishing a secure connection between the client and proxy
14 systems;

15 sending a request to the proxy system for a secure end-to-end
16 connection with the server system;

17 and

18 downgrading the secure connection between the client system and the
19 proxy system to be insecure after the secure end-to-end connection with the
20 server system is established.

1 49. A computer program product as recited in claim 48, the method comprised
2 further of machine-executable instructions for performing the acts of:

3 receiving an authenticate challenge from the proxy system; and
4 sending proper authentication credentials to the proxy system.

5
6 50. A computer program product as recited in claim 49 wherein the authenticate
7 challenge received by the client system is one of a basic and a digest authenticate challenge.

8
9 51. A computer program product as recited in claim 48, the method comprised
10 further of machine-executable instructions for performing the act of receiving a certificate
11 from the proxy system, wherein the certificate may be used to verify the identity of the
12 proxy system.

13
14 52. A computer program product as recited in claim 48 wherein at least one of
15 the secure client-proxy connection and the secure end-to-end connection is certificate based.

16
17 53. A computer program product as recited in claim 52 wherein at least one of
18 the secure client-proxy connection and the secure end-to-end connection is one of a secure
19 sockets layer and a transport layer security connection.

20
21 54. A computer program product as recited in claim 48, the method comprised
22 further of machine-executable instructions for performing the act of sending proper
23 authentication credentials to the proxy system, wherein the proper authentication credentials
24 sent to the proxy system are certificate based.

1 55. A computer program product as recited in claim 48, the method comprised
2 further of machine-executable instructions for performing the act of transferring data
3 between the client system and the server system through the secure end-to-end connection.

4

5 56. A computer program product as recited in claim 48, the method comprised
6 further of machine-executable instructions for performing the act of setting the cipher set for
7 the secure client-proxy connection to be a null cipher, thereby downgrading the client-proxy
8 connection to be insecure.

9

10 57. A computer program product as recited in claim 48 wherein the request for a
11 secure end-to-end connection comprises a hypertext transfer protocol connect request.

12

13 58. A computer program product as recited in claim 48 wherein the server system
14 comprises one of a reverse proxy server system and a forward proxy server system.

15

16 59. A computer program product as recited in claim 48 wherein at least one
17 connection is over the Internet.

18

19 60. A computer program product as recited in claim 48 wherein the server system
20 comprises a cascaded proxy system, the server system allowing secure connections, insecure
21 connections, or both secure and insecure connections, with one or more other server
22 systems.